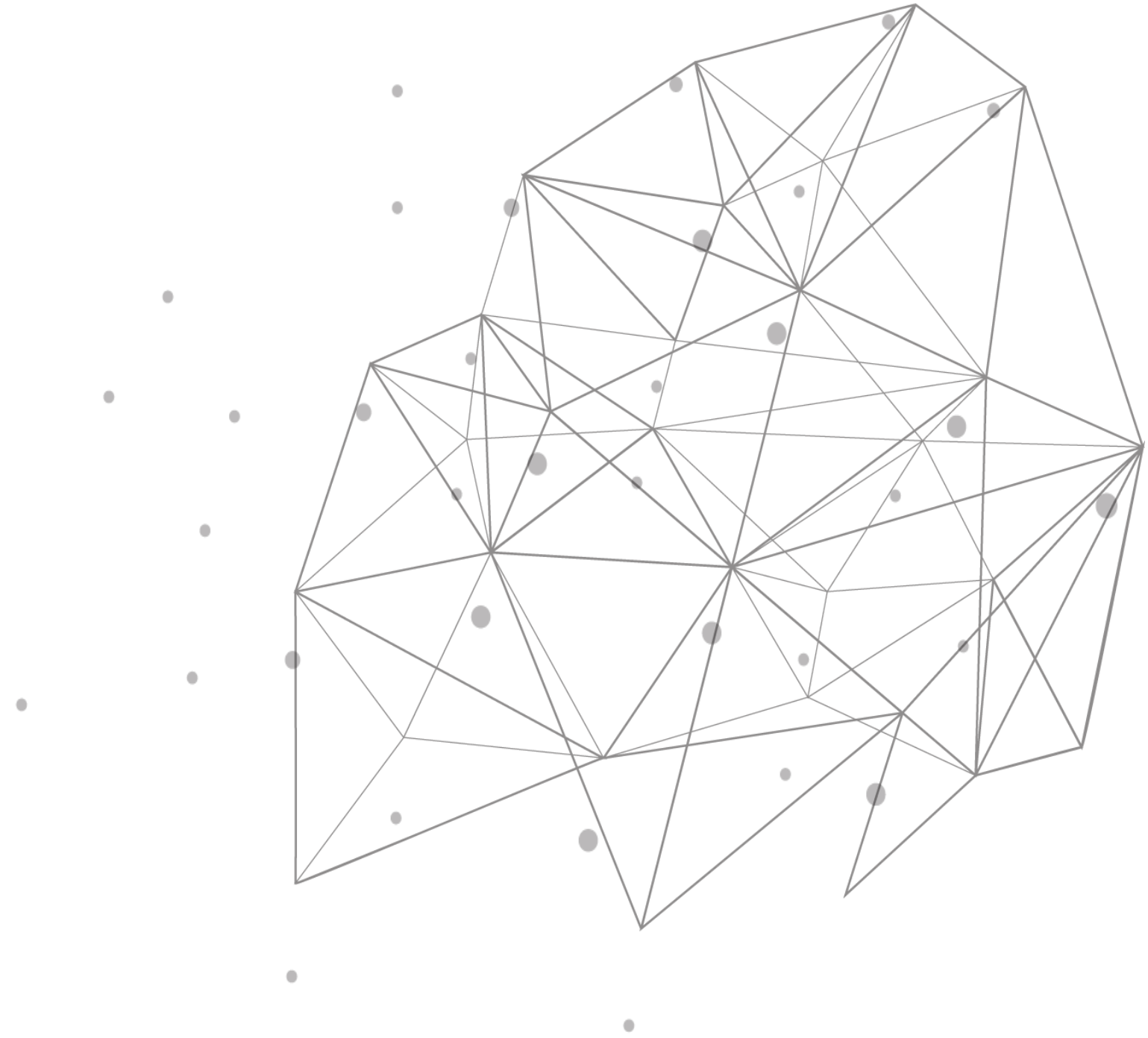
TCPWave DDI

White Paper



Introduction

Enterprises are growing more dispersed, borderless, developing, and deploying their applications at a faster rate that needs rapid and secure access to run the business smoothly. To achieve this, enterprises require a one-stop DDI solution that can drive their businesses efficiently through agile, secure, scalable, and reliable infrastructure management.

Gartner Research

TCPWave has been rated as the number one choice by the Gartner research. The latest publication, which can be obtained as a complimentary copy from the TCPWave sales team, clearly shows how modern and agile frameworks used in the product development of TCPWave propels TCPWave into a territory of undisputed leadership.

TCPWave = Agility + Innovation

Business Objectives

The DDI solution provides enterprises with all the necessary tools to have centralized management that supports their ever-growing business requirements. The opted DDI solution must be secure, scalable, and resilient. An ideal DDI solution has the following abilities:

- ✓ Provide a user interface that is intuitive, easy to navigate and responsive to various browsers and devices and extensive API support to integrate with various automation systems such as ServiceNow, VMWare, Microsoft SQL Server as a Service, OpenShift etc. Seamlessly integrate with Microsoft Active Directory.
- ✓ Support segregation of duties so that a single administrator does not have a conflict of user administration and network management.
- ✓ Integrate with cloud providers and manage the cloud hosted DNS such as AWS Route 53, Google DNS, Microsoft Azure DNS, Akamai, Neustar, Cloudflare etc.
- ✓ Support SSL Certificate or Token based authentication for the APIs. Support highest grade of encryption.
- ✓ Provide a configuration assurance that the standards are properly applied to the production environment.
- ✓ Generate performance management reports for risk control self-assessment, audit reports for compliance and automated change reconciliation reports to a global reconciliation team.
- ✓ Detect alerts related to the core network services (DNS and DHCP). To detect and prevent malicious traffic.
- ✓ To make rapid changes without any degradation in the performance. Provide extensive logging capability to assist in network troubleshooting and network forensics.
- ✓ To forward alerts into NetCool, Tivoli, EMC Smarts etc.
- ✓ Support machine learning algorithms for detecting BotNets and malware. Data infiltration and exfiltration attempts must be detected and reported. Support both IPv4 and IPv6 networks.

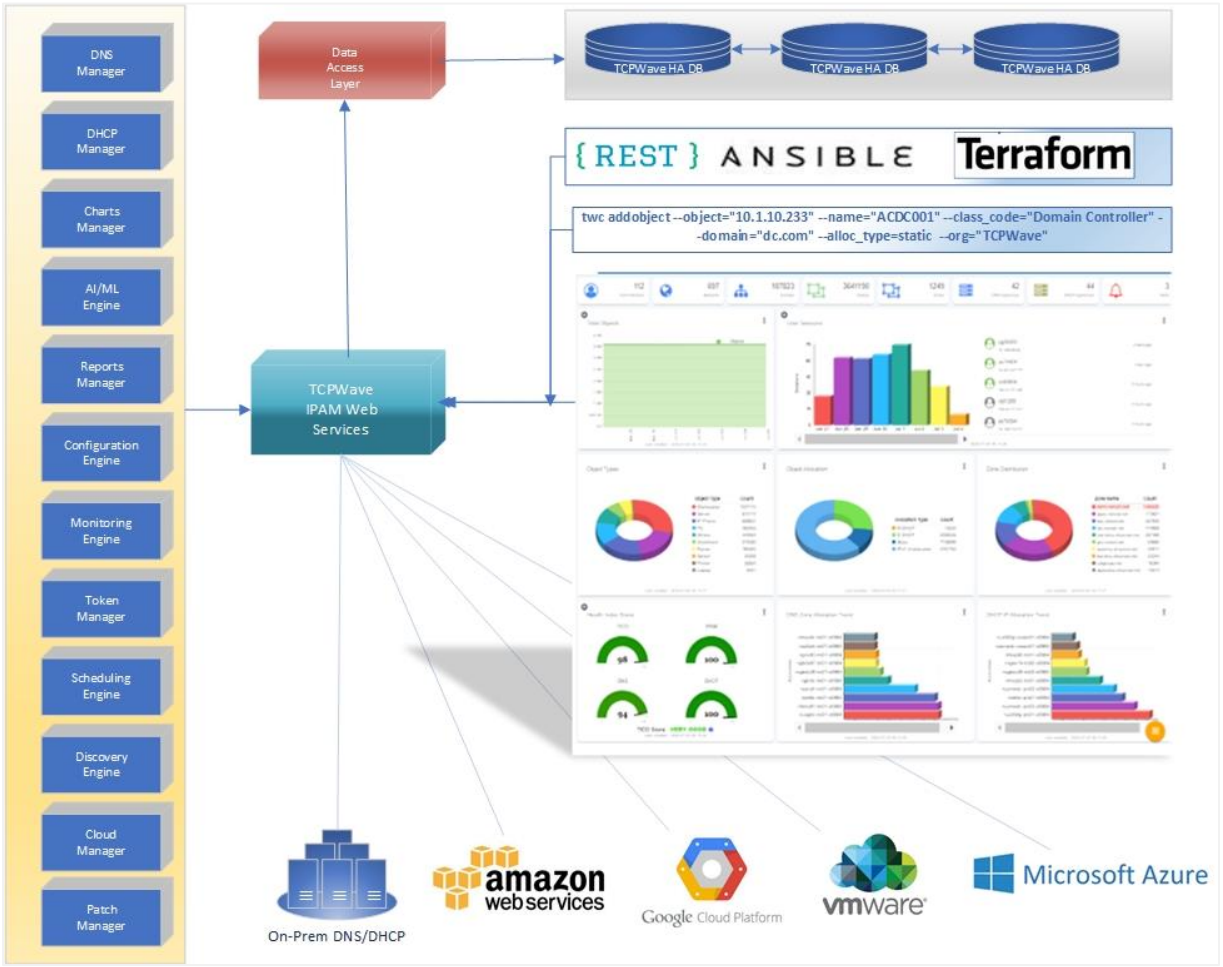
TCPWave as Enterprise DDI Platform

TCPWave's enterprise DDI platform helps you to move from traditional DDI solutions to modern DDI solution that can deliver the scalability**,** security, performance, and resilience required by modern infrastructure**.**

- ✓ **Friendly User Interface**: The user interface is intuitive and provides a powerful dashboard for viewing various metrics.
- ✓ **Segregation of Duties**: Fully supports segregation of duties. For example, InfoSec User Admins cannot touch DNS/DHCP configs and DNS/DHCP Super Admins cannot add users.
- ✓ **Software Resiliency**: Offers BIND/Yadifa for DNS Master/Slave software resiliency. Offers BIND/Unbound for DNS Cache layer resiliency.
- ✓ **Fault Management**: TCPWave provides a powerful monitoring engine that is built into the product. It provides OS metrics and alerts as a part of the product.
- ✓ **Performance Management**: Provides performance reports within the product. InfoVista Libraries for TCPWave SNMP polling exists.
- ✓ **Audit Reports**: Provides over 50 audit reports that can be emailed at scheduled times in a CSV/PDF format.
- ✓ **Patch Management:** Provides a central interface to deploy patches in a phased manner. Patching can be done over several weeks with logic to roll back added to the scheduler.
- ✓ **Configuration Assurance**: Provides an HPNA driver to capture all TCPWave configs that are uploaded for a daily automated change reconciliation process. Provides the ability to view any config file from Web UI and CLI.
- ✓ **Ease of Migration**: TCPWave provides tools (free of charge) to perform your existing DNS/DHCP data into TCPWave's IPAM. Data migration for 3 million IP data set is done in 4 hours.
- ✓ **Better Security**: TCPWave IPAM leverages T-Message Channel for communications with the remote DNS and DHCP appliances, which is an end to end encrypted channel. TCPWave DNS supports DNSSEC and is immune to Cache poisoning attacks due to its advanced DNS packet filtering firewall system. RestAPI calls from TCPWave management use encrypted tokens for SSL certificate-based authentication. TCPWave IPAM supports GSS-TSIG from multiple AD forests that have no trust.
- ✓ **Cloud Integration**: TCPWave offers the best cloud integration out there with support to multiple cloud platforms. You can not only manage your public cloud DNS but also host TCPWave DNS appliances in your public cloud.
- ✓ **Network Automation**: TCPWave automates the management of your DNS and DHCP services with minimal downtime. The DHCP leases are saved in the management appliances and are instantaneously synced with the DNS appliances.
- ✓ **Worry-Free**: Leverage the TCPWave Anycast routing to set up a robust cluster of DNS appliances.

TCPWave Key Benefits

The primary advantage that the TCPWave provides is the ability to seamlessly manage the DDI infrastructure using REST API calls. The TCPWave IPAM is the only provider in today's DevOps community with 1400+ REST API calls. Other providers are based on legacy technologies such as Perl API or SOAP APIs. TCPWave proudly claims to be the only provider in the market today to integrate with numerous orchestration frameworks such as Terraform, VMware vRA, AWS Lambda, etc. using an SSL certificate as a method of authentication. The other providers use a plain text user name and password to authenticate with their dated APIs. The below figure illustrates a high-level feature set of the TCPWave DDI solution.

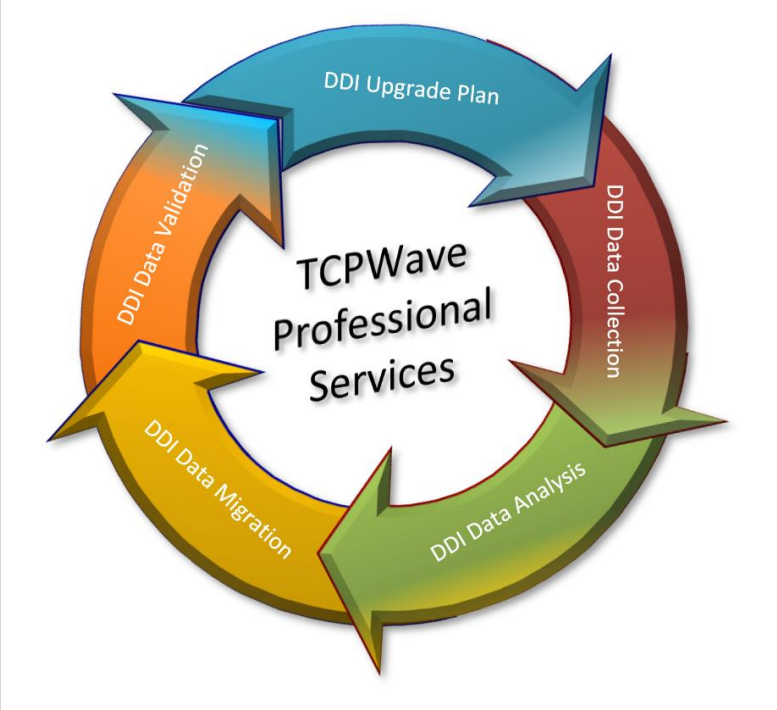


TCPWave Professional Services

TCPWave goes above and beyond to ensure that the DDI migration is performed seamlessly with zero downtime to the enterprise's mission-critical DNS and DHCP infrastructure. Unlike other providers, TCPWave does not provide a one-size-fits-all approach for performing cutovers. After a series of meetings between the professional services team and the enterprise's DDI architects, a carefully designed migration plan is drafted.

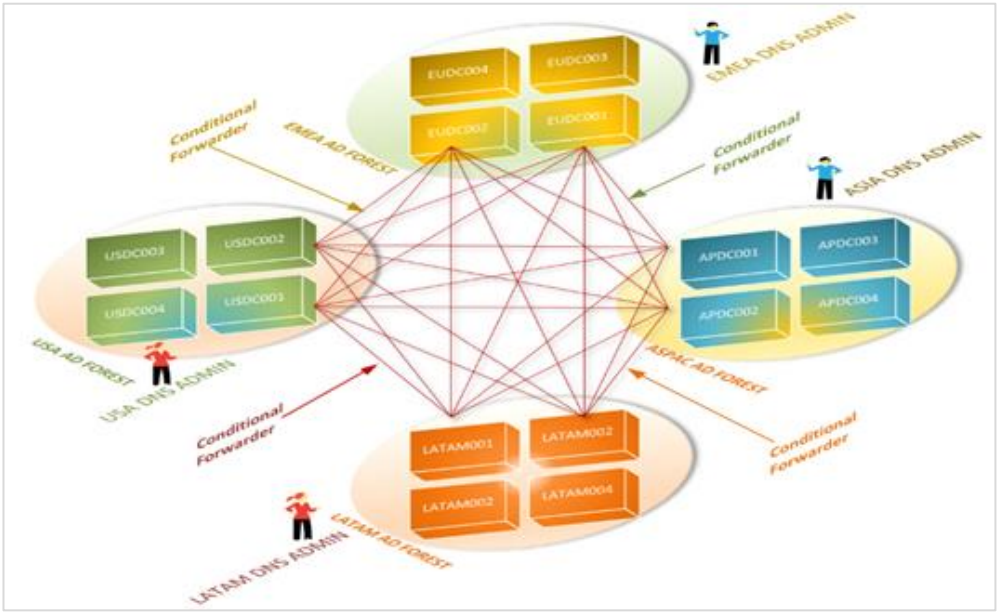
Design changes such as proper placement of the DDI infrastructure, designing and implementing end-to-end monitoring solutions, capacity planning methodology, and config assurance tools are some of the aspects used in the migration planning. Numerous dry runs are performed in a development environment to ensure striking success when deployed in a production environment. Data cleanups, if needed are performed before the migration. The exception reports that provide a delta between the converted dataset to the original dataset are scrutinized. A dedicated Project Manager (PM) and a Technical Account Manager (TAM) are allocated. Weekly communication is scheduled to ensure that proper planning and implementation steps are undertaken before administering a cutover.

The post-migration follow-ups by the TAM ensure that the DDI infrastructure is operating seamlessly after a successful migration. The enterprise's NetOps and DevOps teams are then brought on-board to facilitate an integration using the automation frameworks. TCPWave also provides a training session to improve the operational efficiency of the deployment.



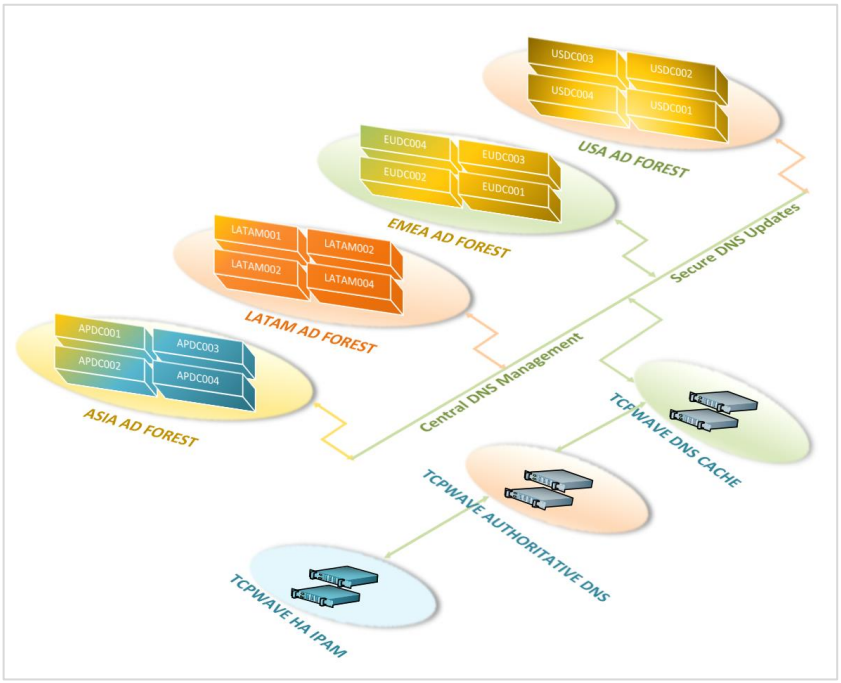
TCPWave Versus Microsoft DNS

Microsoft's Active Directory is a directory service developed by Microsoft and used to store objects like the user, computer, printer, and network information. It is primarily used for authentication and resource management within an active directory domain. The AD infrastructure relies heavily on the DNS infrastructure. It is mandatory to have a one-to-one mapping between an AD forest name to a DNS domain name. The domain controllers self-register their DNS resource records. It is a common misconception that Microsoft's AD requires Microsoft's DNS. The TCPWave DDI management is engineering to seamlessly integrate with Microsoft Active Directory. It can manage large AD environments and it can also add stability by centralizing the DDI management. This whitepaper discusses the most common challenges in a large AD-integrated DNS environment and it also lists the advantages of the TCPWave engineered design that fully supports the integration with active directory.



It is common to see many enterprise-grade deployments utilizing Microsoft's in-built AD integrated DNS. These distributed deployments typically keep growing without following the best practices recommended by TCPWave. The failure to follow a common set of standards across a global infrastructure by a set of different individuals reporting to separate management chains is a reason why a large-scale AD deployment is complex to maintain. The configuration of multiple conditional forwarders makes it extremely difficult to maintain, manage, monitor, scale, and troubleshoot. It is also common to see various large scale AD integrated DNS deployments to have frequent DNS blackouts because of improper designs. As the number of forests and the trusts grow, the environment becomes fragile. The Active Directory trusts require DNS resolution to the root forest, child forests, and possibly some standalone forests depending on the deployment of the AD forests. The resources in one AD domain can be used by the users in another AD domain if the DNS resolution is functioning properly. When data centers move or when a new network topology is designed, a single DNS change in one forest for a re-IP of a set of domain controllers could cause a blackout in other forests if multiple de-centralized administrators do not conduct

the change properly with proper co-ordination. Forwarders will stop to work, and delegations will become lame if all the distributed AD integrated DNS configurations are not updated accordingly.



TCPWave's DDI solution centralizes the DNS management in the enterprise. In the TCPWave managed DDI design, each domain controller will point to a cache-only TCPWave DDI appliance. The cache-only DNS appliances would fetch the DNS answers from the TCPWave authoritative DDI appliances. The TCPWave IPAM, running in a HA (High Availability) mode, will manage the authoritative and the cache DNS appliances. Each domain controller in each AD forest would update the authoritative DNS zone that is hosted on the TCPWave authoritative DDI remote. The TCPWave IPAM can configure an IP based ACL to accept the DNS updates from the domain controllers. Since a UDP based update controlled with an IP based ACL is subject to spoofing or hijacking, TCPWave goes one step further and secures the DNS update using GSS-TSIG. GSS-API algorithm uses Kerberos for passing security tokens to provide authentication, integrity, and confidentiality. The web interface of the TCPWave IPAM provides a simplified method to manage the Kerberos configurations, Service Principal Names (SPN), secure DNS update policies, TSIG keys, etc. across all the AD-enabled DNS zones. The TCPWave design provides a seamless AD integration with auditing, reporting, disaster recovery, monitoring, role-based access control, and many more features.

Why TCPWave approach is better and scalable?

TCPWave has the experience and the global reach, to help you efficiently deploy your network when growing, upgrading, or changing network elements.

- TCPWave provides the skills to help you smoothly install a global network, as well as the ability to leverage partnerships to reduce deployment costs.
- Provides Support Assistance and Professional Services related to DNS, DHCP, IPAM.
- Different groups have diverse requirements for enterprise support & TCPWave offers support contracts.

- TCPWave support contracts cover issues related to software installation, maintenance, updates, configuration, logging, and troubleshooting, generic questions.
- TCPWave support covers TCPWave IPAM installation, configuration, and handover of the administrative responsibilities to your support personnel.

Conclusion

Legacy DDI providers that were designed in the late 90s or the early 2000s cannot keep up with today's demanding needs of the DevOps and CloudOps communities. The stringent information security standards of the enterprises require proper segregation of duties, role-based access controls, and the use of SSL certificates for all API communication. The outdated systems that use weak ciphers in their encryption algorithms cannot be used in today's automation frameworks. A centralized management model with linear scalability delivered to the global data centers is a critical decision-making factor. Open-source systems, native ISC's BIND/DHCP, Microsoft's DNS/DHCP, and excel spreadsheets are things of the past since they cannot cater to the needs of automation. Customers are advised to carefully evaluate the pros and cons of the available DDI management choices, the information security recommendations, capital expenditures (CAPEX) and operating expenses (OPEX), the quality of professional services, design oversights of the current implementation, etc and make a business decision that best suits the franchise critical DDI framework of your enterprise.

TCPWave is a core network development company that delivers a full suite of cloud and on-prem DDI solutions with advanced edge over internet security employing innovative technologies and agile approaches.

Corporate Headquarters | 600 Alexander Road | Princeton, NJ | 08540
888.831.8276 | support@tcpwave.com | www.tcpwave.com
TCPWave Inc.